(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 61 403 A 1**

(51) Int. Cl.[7]: G 07 C 9/00

(21) Aktenzeichen: 199 61 403.2
(22) Anmeldetag: 20. 12. 1999
(43) Offenlegungstag: 2. 8. 2001

DE 199 61 403 A 1

(66) Innere Priorität:
199 57 283. 6 19. 11. 1999

(71) Anmelder:
Accenture Dienstleistungen GmbH, 65843 Sulzbach, DE

(74) Vertreter:
BOEHMERT & BOEHMERT, 28209 Bremen

(72) Erfinder:
Hellenthal, Markus, 56154 Boppard, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) System und Verfahren zur automatisierten Kontrolle des Passierens einer Grenze

(57) System und Verfahren zur automatisierten Kontrolle des Passierens einer Grenze mit einer Personendatenerfassungseinrichtung, einer Biometriedatenerfassungseinrichtung, einer Personendatenweitergabeeinrichtung, einer Datenspeichereinrichtung, einer Durchgangsschleuse, einer Vereinzelungseinrichtung, einer Datenleseeinrichtung, einer Echtheitsüberprüfungseinrichtung, einer Datenmanipulationsüberprüfungseinrichtung, einer Einrichtung zum Öffnen des Eingangs der Durchgangsschleuse, einer Biometriedatenerfassungseinrichtung, einer Vergleichseinrichtung, einer Alarmauslöseeinrichtung, einer Personendatenweitergabeeinrichtung und einer Einrichtung zum Öffnen des Ausgangs der Durchgangsschleuse und ein Verfahren zur automatisierten Kontrolle des Passierens einer Grenze.

DE 199 61 403 A 1

BNSDOCID: <DE_____19961403A1_I_>

Beschreibung

Die vorliegende Erfindung betrifft ein System und ein Verfahren zur automatisierten Kontrolle des Passierens einer Grenze.

Grenzkontrollen z. B. an Flughäfen, aber auch im Bereich der Land- und Fährverkehre sind für den grenzüberschreitenden Personenverkehr zeitkritisch. Gleichzeitig ist der Aufwand der Kontrollbehörden – unter anderem wegen des Schengener Abkommens in den vergangenen Jahren überproportional zur Anzahl der Reisenden gestiegen. Die seit Jahren steigende Mobilität der Menschen und wachsende Passagierzahlen im internationalen Flugverkehr führen zu neuen Anforderungen im Personenbeförderungswesen. Andererseits sind die personellen und finanziellen Ressourcen der staatlichen Kontrollbehörden, der Luftverkehrsunternehmen und der Flughafenbetreiber sowie die räumlichen Gegebenheiten auf vielen internationalen Verkehrsflughäfen zunehmend begrenzt.

Der Erfindung liegt somit die Aufgabe zugrunde, die Geschwindigkeit des Passagierverkehrs zu erhöhen.

Erfindungsgemäß wird diese Aufgabe gelöst durch ein System zur automatisierten Kontrolle des Passierens einer Grenze, mit:

- einer Einrichtung zur Erfassung von Personendaten von Systembenutzern,
- einer Einrichtung zur Erfassung von biometrischen Daten der Systembenutzer,
- einer Einrichtung zur Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank und Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,

einer Einrichtung zum Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,

- einer vor einer Grenze angeordneten Durchgangsschleuse zum Regulieren des Durchgangs der Systembenutzer mit einem Eingang und einem Ausgang, wobei der Eingang und der Ausgang in Grundstellung verschlossen sind,
- einer vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zur Vereinzelung der Systembenutzer, einer hinter der Vereinzelungseinrichtung, aber vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zum Lesen der auf den Identifikationsmedien gespeicherten Daten,
- einer vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zur Überprüfung der Echtheit der Identifikationsmedien,
- einer vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zur Überprüfung des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- einer Einrichtung zum Öffnen des Eingangs der Durchgangsschleuse, wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt wurden,
- einer in der Durchgangsschleuse befindlichen Einrichtung zum Erfassen von biometrischen Daten eines hineingelassenen Systembenutzers,
- einer Einrichtung zum Vergleich der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- einer Einrichtung zum Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- einer Einrichtung zur Weitergabe der Personendaten an die Fahndungsdatenbank und zur Abfrage, ob der Systembenutzer auf einer Fahndungsliste steht, und
- einer Einrichtung zum Öffnen des Ausgangs der Durchgangsschleuse und Ermöglichen eines Grenzübertritts des Systembenutzers, wenn das Ergebnis der Fahndungsabfrage negativ ist, und zur Auslösung eines Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

Weiterhin wird die Aufgabe gelöst durch ein Verfahren zur automatisierten Kontrolle des Passierens einer Grenze, das die folgenden Schritte umfaßt:

- Erfassen von Personendaten von Systembenutzern,
- Erfassen von biometrischen Daten der Systembenutzer,
- Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank und Vornahme einer Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,
- Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,

Vereinzelung der einen Grenzübertrittsversuch unternehmenden Systembenutzer vor einer Durchgangsschleuse mit einem Eingang und einem Ausgang, wobei der Eingang und der Ausgang in Grundstellung geschlossen sind,

- Lesen der auf dem Identifikationsmedium gespeicherten Daten,
- Überprüfung der Echtheit des jeweiligen Identifikationsmediums,
- Überprüfen des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- Öffnen des Eingangs der Durchgangsschleuse, wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt werden,
- Erfassen von biometrischen Daten eines in die Durchgangsschleuse hineingelassenen Systembenutzers,
- Vergleichen der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- Weitergeben der Personendaten an die Fahndungsdatenbank und Abfragen, ob der Systembenutzer auf einer Fahndungsliste steht, und
- Öffnen des Ausgangs der Durchgangsschleuse, wenn das Ergebnis der Fahndungsabfrage negativ ist, bzw. Auslösen eine Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

Insbesondere kann bei dem System vorgesehen sein, daß die Einrichtung zur Erfassung von Personendaten von Sy-

BNSDOCID: <DE_____19961403A1_I_>

stembenutzern eine Einrichtung zum automatischen Einlesen der Personendaten aufweist. Beispielsweise kann die Einrichtung zum automatischen Einlesen der Personendaten ein Scanner sein.

Vorteilhafterweise umfaßt die Einrichtung zur Erfassung von biometrischen Daten eine Einrichtung zur Erfassung eines Fingerabdruckes und/oder der Netzhautstruktur und/oder der Gesichtsmerkmale und/oder der Stimme und/oder Sprache eines jeweiligen Systembenutzers.

Eine weitere besondere Ausführungsform des Systems ist gekennzeichnet durch eine Einrichtung zur Verarbeitung der erfaßten biometrischen Daten und Umrechnung in ein oder mehrere repräsentative(s) Datenmerkmal(e), anhand dessen/derer eine Wiedererkennung des Systembenutzers bei der Kontrolle möglich ist.

Auch kann vorgesehen sein, daß die Einrichtung zur Speicherung von Daten eine Einrichtung zur Verschlüsselung der Personen- und/oder Identifikationsmediumdaten und zur Erzeugung eines identifikationsmediumspezifischen Schlüssels aufweist.

Ferner kann auch vorgesehen sein, daß die Verschlüsselungseinrichtung ein lokal vorgesehenes Sicherheitsmodul ist oder sich in einem Hintergrundsystem befindet, das über eine On-Line-Datenverbindung verbunden ist.

Vorzugsweise weist die Einrichtung zur Speicherung der Daten eine Einrichtung zur elektrischen Personalisierung der verschlüsselten Daten in dem Identifikationsmedium und/oder eine Einrichtung zum Aufbringen der Personendaten und gegebenenfalls eines Fotos sowie der Unterschrift des jeweiligen Systembenutzers auf das Identifikationsmedium auf Beispielsweise können die Personendaten im Thermotransfer-Druck auf das Identifikationsmedium aufgebracht werden.

Günstigerweise weist die Einrichtung zur Speicherung der Daten eine Einrichtung zum Überziehen des Identifikationsmediums mit einer Laminatfolie auf. Durch die Laminatfolie wird das Identifikationsmedium fälschungssicher.

Vorzugsweise sind die Identifikationsmedien Smart Cards.

Günstigerweise ist in der Durchgangsschleuse mindestens eine Videokamera vorgesehen. Dies ermöglicht eine Überwachung der Durchgangsschleuse insbesondere hinsichtlich der Vornahme einer wirksamen Vereinzelung.

Weiterhin kann vorgesehen sein, daß die Einrichtung zum Lesen der auf den Identifikationsmedien gespeicherten Daten eine Einrichtung zum Berechnen des identifikationsmediumspezifischen Schlüssels aus den verschlüsselten Identifikationsmediumdaten und Verifikation desselben aufweist. Damit ist die Vornahme einer Kartenlegitimationsprüfung möglich.

Weiterhin weist die Einrichtung zum Lesen der auf dem Identifikationsmedium gespeicherten Daten vorzugsweise eine Einrichtung zum Entschlüsseln der verschlüsselten Personendaten und Verifikation derselben auf. Dies ermöglicht eine Personenlegitimationsprüfung.

Eine weitere besondere Ausführungsform der Erfindung ist gekennzeichnet durch eine Einrichtung zur Erzeugung und Verteilung von Schlüsseln für die Datenverschlüsselungen und Überwachung des Systembetriebes. Eine derartige Einrichtung erfüllt die Funktion eines Trust Center.

Eine weitere besondere Ausführungsform der Erfindung ist gekennzeichnet durch eine Einrichtung zur Verwaltung und Überwachung insbesondere der Lebensdauer aller an Systembenutzer ausgegebener Identifikationsmedien.

Schließlich ist eine weitere besondere Ausführungsform der Erfindung gekennzeichnet durch eine Einrichtung zur kryptographischen Verschlüsselung von zwischen Einrichtungen des Systems und/oder zwischen dem System und externen Einrichtungen übertragenen Daten. Dies soll vor einem unerlaubten Zugriff auf die übertragenen Daten schützen.

Die Unteransprüche 17 bis 26 betreffen vorteilhafte Weiterentwicklungen des erfindungsgemäßen Verfahrens.

Der Erfindung liegt die überraschende Erkenntnis zugrunde, daß durch eine Integration der behördlichen Kontrollen in den Gesamtablauf, wobei ein Teil der Kontrolle im Prinzip vorgezogen wird, eine Beschleunigung und Vereinfachung der Abwicklung des Grenzverkehrs erzielt wird, ohne daß darunter die Qualität der Kontrolle leidet. Durch die zumindest zum Teil vorgezogene Kontrolle kann die Kontrolle an der Grenze hinsichtlich der bereits vorab kontrollierten, unproblematischen Reisenden vereinfacht und verkürzt werden, wodurch eine Konzentration der Polizei- und Kontrollkräfte auf potentielle Täter und Gefahren möglich wird.

Die vorab durchgeführte Kontrolle erlaubt eine maschinelle Überprüfung des polizeilich unproblematischen grenzüberschreitenden Reisendenverkehrs mit all den Einzelkomponenten, die auch eine Grenzkontrolle durch Polizeibeamte beinhaltet, nämlich Personenvergleich, Echtheitsprüfung von Grenzübertrittsdokumenten, Fahndungsabfrage, Gestattung des Grenzübertritts. Dabei werden unter Berücksichtigung aller nationalen, Schengener und EU-Anforderungen zuvor aus polizeilicher Sicht unproblematische eingestufte Reisende nach Antragstellung und auf freiwilliger Basis mittels auf ihren Identifikationsmedien gespeicherten Personendaten und biometrischen Daten beim Grenzübertritt jeweils aktuell maschinell identifiziert und über eine On-Line-Fahndungsabfrage polizeilich überprüft.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den Ansprüchen und aus der nachstehenden Beschreibung, in der ein Ausführungsbeispiel anhand der schematischen Zeichnungen im einzelnen erläutert ist. Dabei zeigt:

Fig. 1 eine Draufsicht eines Teils eines Systems gemäß einer besonderen Ausführungsform der vorliegenden Erfindung; und

Fig. 2 schematisch wesentliche Einrichtungen und Einrichtungsblöcke des Systems;

Fig. 1 zeigt eine Draufsicht eines Teils eines Systems gemäß einer besonderen Ausführungsform der Erfindung. Der gezeigte Teil betrifft die Kontrolle von Systembenutzern direkt an einer Grenze (z. B. Landesgrenze). **Fig.** 1 zeigt eine Durchgangsschleuse **10** mit einem Eingang **12** und einem Ausgang **14**. Der Eingang **12** und der Ausgang **14** sind jeweils mit einer Drehtür **16** bzw. **18** versehen. Vor der Drehtür **16** am Eingang **12** befindet sich eine Einrichtung zur Vereinzelung der Systembenutzer (nicht gezeigt). Die Vereinzelung kann mechanisch, aber auch z. B. optisch durchgeführt werden. Beispielsweise kann dazu eine Ampel verwendet werden. Wenn die Ampel auf Grün steht, darf eine einzelne Person passieren. Wenn eine Person bei Rot weitergeht, wird ein optischer und/oder akustischer Alarm ausgelöst. Zwischen dieser Einrichtung und der Drehtür **16** befindet sich ein Kartenlesegerät **20** zum Lesen von Smart Cards. Die Drehtür **16** ist in Grundstellung arretiert und verschließt somit den Eingang **12**. In der Durchgangsschleuse **10** befindet sich ein Biometriedatenlesegerät **22**. Das Kartenlesegerät **20** und das Biometriedatenlesegerät **22** sind mit einem lokalen Server des Bundesgrenzschutzes (nicht gezeigt) verbunden. In der Durchgangsschleuse **10** befindet sich darüber hinaus noch eine Videokamera **24** zur Überwachung der mechanischen Vereinzelung der Systembenutzer.

In **Fig.** 2 sind schematisch die wesentlichen Einrichtungen einzeln bzw. in Blöcken des Systems gezeigt. Ein Systemblock, der mit dem Bezugszeichen **26** versehen ist, be-

BNSDOCID: <DE_____19961403A1_I_>

trifft die Beantragung und Ausgabe einer Karte (sogenanntes Enrolment Center). Die Karte in Form einer Smart Card **28** dient als Berechtigungsausweis für jeden Systembenutzer. Sie wird beim Grenzübertritt in dem in **Fig. 1** gezeigten Teil des Systems, der hier als dezentrales automatisiertes Grenzkontrollsystem **30** bezeichnet ist, überprüft. Das dezentrale automatisierte Grenzkontrollsystem **30** umfaßt einen lokalen Server des Bundesgrenzschutzes, der über einen Dienststellen-Server **32** des Bundesgrenzschutzes mit einer Fahndungsdatenbank **34** der INPOL, einem Trust Center **36**, einer zentralen Datenverwaltungseinrichtung **38** des Bundesgrenzschutzes und dem Enrolment Center **26** in Verbindung steht.

In dem Enrolment Center **26** kann eine Kartenbeantragung vorgenommen werden. Diese umfaßt alle Prozeßschritte, die zur Erfassung der potentiellen Systembenutzer, also insbesondere die Erfassung ihrer Personen- und biometrischen Daten, notwendig sind. Es können mehrere Enrolment Center vorgesehen sein, die an verschiedenen Orten errichtet sind. Zur Kartenbeantragung legen die potentiellen Systembenutzer ihr Grenzübertrittsdokument vor, von dem der Bediener eines PCs, auf dem die Erfassungssoftware läuft, die Daten automatisch oder manuell erfaßt. Der Datensatz wird auf einem Formblatt ausgedruckt und vom antragstellenden, potentiellen Systembenutzer unterschrieben. Das Formblatt enthält unter anderem folgende weitere Angaben:

- eine Beschreibung des Systems,
- die Personalien des potentiellen Systembenutzers,
- die Bedingungen für die freiwillige Teilnahme am System,
- die notwendigen datenschutzrechtlichen Erklärungen zur Erhebung, Speicherung, Übermittlung und Verarbeitung der Personendaten des antragstellenden, potentiellen Systembenutzers im Zusammenhang mit der automatisierten Grenzkontrolle,
- einen Hinweis auf die Pflicht des Systembenutzers, bei jedem Grenzübertritt ein gültiges Grenzübertrittsdokument mit sich zu führen, und
- Hinweise zu den anerkannten Reisezwecken, für die das System genutzt werden darf.

In einem nächsten Schritt wird der Fingerabdruck des potentiellen Systembenutzers mittels eines Fingerabdrucklesegerätes (nicht gezeigt) erfaßt. Die vom Fingerabdrucklesegerät gewonnen Daten werden durch die Verarbeitungssoftware in ein oder mehrere repräsentative Datenmerkmale umgerechnet, anhand derer eine Wiedererkennung des Systembenutzers bei der Grenzkontrolle möglich wird. Dann wird ein Test auf Duplikate vorgenommen, das heißt es wird überprüft, ob der Antragsteller bereits im System erfaßt ist. Die zuvor erfaßten Personendaten werden um die biometrischen Daten ergänzt und zur Verschlüsselung gegeben. Diese erfolgt entweder am lokalen System in einem dafür vorgesehenen Sicherheitsmodul oder in einem Hintergrundsystem, zu welchem für diesen Zweck eine On-Line-Datenverbindung geschaltet wird. Die verschlüsselten Daten werden im Enrolment Center in einen Smart Card-Rohling elektrisch personalisiert und die Personendaten auf dem Smart-Card-Körper im Thermotransfer-Druck aufgebracht. Zusätzlich können gegebenenfalls ein Foto des Systembenutzers sowie seine Personalien (beides erforderlichenfalls als Grundlage für eine manuelle Überprüfung, z. B. im Rahmen von Stichprobenkontrollen), seine Unterschrift und der Name des ausstellenden Enrolment Centers aufgedruckt werden. Anschließend wird der Smart-Card-Körper mit einer fälschungssicheren Laminatfolie überzogen. All diese Schritte laufen in einer Maschine ab und werden vom PC überwacht. Nach einer Funktionskontrolle an einem Terminal im Enrolment Center wird die Smart Card dem Systembenutzer ausgehändigt. Das gesamte Enrolment dauert weniger als 10 Minuten. Die Kartenbeantragung und -ausgabe kann auch gleichzeitig mit der erstmaligen Benutzung des Systems an der Grenze vor Ort vorgenommen werden.

Alle hoheitlichen Schritte – die Durchführung der vorgezogenen Grenzkontrolle entsprechend der nationalen, Schengener und EU-Anforderungen und die Freigabe der Smart Card – sind einem Beamten der Grenzkontrollbehörde vorbehalten. Er wird gegebenenfalls unterstützt durch Personal bzw. Beauftragte des Betreibers. Für die Mitarbeiter in den Enrolment Center werden ebenfalls geeignete Zugangskontrollen vorgesehen.

Darüber hinaus stellt die Erfassungssoftware sicher, daß Smart Cards nur mit Zutun legitimierter Grenzkontrollbeamter, nur nach erfolgreichem Verlaufen aller erforderlichen Schritte und nur für visumsbefreite Angehörige bestimmter zugelassener Staaten ausgestellt werden, die im Besitz eines gültigen Reisedokumentes sind.

Die Kartenkontrolle umfaßt alle Prozesse, die bei der Prüfung des Karteninhabers im Rahmen der Einreise durchgeführt werden. Die Kartenkontrolle findet innerhalb einer Durchgangsschleuse **10** (siehe **Fig. 1**) statt, welche die zu kontrollierende Person betreten muß.

Die Durchgangsschleuse selbst kann problemlos in die bestehende Infrastruktur integriert werden, das heißt es sind nur geringfügige bauliche Veränderungen notwendig. Der lokale Server dient zur Ablaufsteuerung und zur Kommunikation mit externen Rechnern.

Vor der Durchgangsschleuse **10** findet zunächst eine mechanische Vereinzelung mittels einer Einrichtung zur mechanischen Vereinzelung (nicht gezeigt) statt, um das Eintreten von Unberechtigten sowie mehreren Personen zur gleichen Zeit zu verhindern. Diese Maßnahme wird durch den Einsatz einer Videokamera **24** in der Durchgangsschleuse **10** und entsprechender Bildauswertungssoftware ergänzt.

Hinter der Einrichtung zur Vereinzelung, aber vor dem Eingang **12** wird die zu überprüfende Person zum Einführen der Smart Card in ein Kartenlesegerät **20** aufgefordert. In dem Kartenlesegerät **20** befindet sich ein Sicherheitsmodul (nicht gezeigt) zur Echtheitsüberprüfung der Smart Card sowie der darauf gespeicherten Personendaten. Jede authentische Smart Card besitzt einen Smart Card-spezifischen Schlüssel, der basierend auf bestimmten Smart Card Daten von dem Sicherheitsmodul im Kartenlesegerät **20** berechnet und sodann verifiziert werden kann. Die Kommunikation zwischen der Smart Card und dem Sicherheitsmodul in dem Kartenlesegerät **20** wird zusätzlich mit einem temporären Schlüssel geschützt, der vorher zwischen der Smart Card und dem Sicherheitsmodul ausgehandelt worden ist.

Danach werden die Personendaten einschließlich biometrischen Daten aus der Smart Card gelesen und eine angehängte Signatur (MAC) mit Hilfe des öffentlichen Schlüssels im Sicherheitsmodul auf Echtheit überprüft. So können illegale Datenmanipulationen sicher erkannt werden.

Wenn die Echtheit der Karte und das Vorliegen keiner Datenmanipulation verifiziert worden sind, läßt sich die Drehtür **16** drehen, so daß die Person in die Durchgangsschleuse gelangen kann. In der Durchgangsschleuse **10** wird mittels des Biometriedatenlesegerätes **22** der Fingerabdruck des Systembenutzers erhoben und ein Vergleich mit den auf seiner Smart Card gespeicherten biometrischen Daten vorgenommen. Dazu werden aus den lokal gewonnen Daten Extrakte gebildet und mit den in der Smart Card gespeicherten Datenmerkmalen verglichen.

Durch dieses zweistufige Überprüfungsverfahren am Eingang der Durchgangsschleuse und innerhalb derselben wird zweierlei erreicht:

- es wird festgestellt, daß es sich bei der Person, der aufgrund der am Eingang der Durchgangsschleuse geprüften Smart Card der Einlaß gewährt wurde, um einen berechtigten Systembenutzer handelt;
- unberechtigten Personen wird der Eintritt in die Durchgangsschleuse verwehrt; hier dürfte es ausreichen, auf einem Bildschirm am Kartenlesegerät am Eingang der Durchgangsschleuse einen Hinweis zu geben, sich der regulären Grenzkontrolle zu unterziehen.
- Mißbräuchliche Benutzer oder durch das System fälschlicherweise zurückgewiesene Berechtigte (dies läßt sich durch kein technisches System zu 100% ausschließen) werden spätestens in der Durchgangsschleuse zuverlässig festgestellt. Hier wäre – nach einer entsprechenden automatischen Alarmauslösung durch das System – ein Eingreifen durch die Grenzkontrollbehörde oder einen Beauftragten erforderlich, um die Person aus der Durchgangsschleuse zu befreien und einer regulären Grenzkontrolle zuzuführen.

Im nächsten Schritt werden die erforderlichen Personendaten über den lokalen Server des Bundesgrenzschutzes zur Überprüfung an eine Fahndungsdatenbank der INPOL weitergeleitet.

Wenn alle vorab beschriebenen Schritte beanstandungslos durchlaufen werden, wird der Ausgang der Durchgangsschleuse freigegeben. Im Falle einer Beanstandung oder eines fehlerhaften Verhaltens des System wird ein Alarm ausgelöst und mit der Überprüfung der Person durch Personal des Bundesgrenzschutzes fortgefahren.

Die Gestaltung der Durchgangsschleuse, die Art der verwendeten Vereinzelungstechnik und der Freigabe am Ausgang der Durchgangsschleuse können in Abhängigkeit von z. B. der Ergonomie und der Führung großer Verkehrsströme bestimmt werden.

Das Trust Center **36** dient als zentrale Systemkomponente zur Verwaltung aller sicherheitsrelevanten Aspekte des Systems, also insbesondere zur Erzeugung und Verteilung von Schlüsseln und Überwachung des laufenden Systembetriebes.

Die zentrale Datenverwaltungseinrichtung **38** des Bundesgrenzschutzes dient zur Verwaltung aller ausgegebenen Smart Cards mit Funktionen zur Überwachung des Card Life Cycle. Die Kartenverwaltung beinhaltet auch die Funktionen zur Antragsbearbeitung, also der Erfassung der Personendaten und der biometrischen Daten.

Die besondere Sensibilität der Daten der Smart Cards und der damit verbundenen Funktionalität erfordern ein hohes Maß an Schutz gegen:

- Verfälschung der Personendaten auf der Smart Card
- Verfälschung der biometrischen Daten
- Verfälschung der Verbindung zwischen biometrischen Daten und den Personaldaten
- Manipulationen an einem Kontrollterminal
- Manipulationen bei der Erfassung der Personendaten bzw. der biometrischen Daten und
- Angriffe auf die kryptographischen Funktionen im System.

Zur umfassenden Absicherung dieser Risiken ist eine schalenartige Sicherheitsarchitektur zur Absicherung zentraler Informationen und Funktionen ratsam. Ziel der Architektur ist, die Errichtung mehrerer Hürden; die ein potentieller Angreifer überwinden muß, um das System zu manipulieren.

Den Kern bilden die Personendaten zusammen mit den biometrischen Daten. Diese Daten werden im System als eine Einheit betrachtet, das heißt biometrische Daten sind ein Element des Personendatensatzes. Über den Personendatensatz wird zunächst mit Hilfe eines Secure Hash-Verfahrens, z. B. dem SHA-1 Algorithmus, eine kryptographische Prüfsumme erzeugt. Dieser 160 Bit lange Wert hat die typischen Eigenschaften eines guten Hash-Algorithmus, das heißt, er ist im wesentlichen kollisionsfrei. Das Ergebnis des Algorithmus wird als ein Teil der Kryptogrammbildung verwendet, da der gesamte Personendatensatz als Eingabedatum der Verschlüsselung zu groß ist. Der Hash-Wert komprimiert den Inhalt des Personendatensatzes auf eine stark reduzierte Form. Dabei kann vom Hash-Wert nicht auf die ursprünglichen Daten geschlossen werden. Änderungen im Personendatensatz ergeben zwangsläufig eine Änderung im Hash-Wert. Das Secure Hash-Verfahren ist kein Verschlüsselungsverfahren, das heißt, es verwendet keine Schlüssel.

In der zweiten Schale werden wesentliche Extrakte aus den Personendaten (z. B. Name, Geburtsdatum und Geburtsort), insbesondere also die Daten für die Abfrage bei der INPOL-Fahndungsdatenbank, zusammen mit dem Hash-Wert mit einem Private Key-Verfahren verschlüsselt. Als Private Key-Verfahren sollen – abhängig von der weiteren Detailabstimmung – RSA mit einer Schlüssellänge von mindestens 1.024 Bit oder elliptische Kurven mit hinreichender Schlüssellänge genutzt werden.

Für die Verschlüsselung des Extraktes wird der private Schlüssel einer Ausgabestelle oder der private Schlüssel einer zentralen Instanz verwendet. Im letzteren Fall muß der Personendatensatz zur Verschlüsselung an die zentrale Instanz versandt werden und er kann erst dann in die Smart Card personalisiert werden (z. B. durch On-Line-Anfrage).

Für die Entschlüsselung des Extraktes wird der öffentliche Schlüssel benötigt. Dieser wird in den Kontrollterminals hinterlegt. Eine Entschlüsselung liefert zunächst die Personendaten für die INPOL-Abfrage und den Hash-Wert. Der Hash-Wert wird mit einem erneut berechneten Hash-Wert verglichen. Bei Gleichheit kann von einem unverfälschten Datensatz ausgegangen werden.

Innerhalb des Verfahrens sind eine Reihe von Varianten möglich, deren Nutzung von den konkreten Rahmenbedingungen abhängt:

- Eine eindeutige Smart Card-Nummer könnte in den Personendatensatz aufgenommen und dadurch mit diesem verknüpft werden. Eine Übertragung der Daten auf ein andere Smart Card wäre damit nicht möglich. Eine sinnvolle Nutzung dieser Option setzt eine On-Line-Personalisierung voraus, bei der Personendaten und die Smart Card-Nummer verschlüsselt und direkt in die Smart Card personalisiert werden.
- Die Verschlüsselung des Personendatensatzes kann mit dem privaten Schlüssel der Ausgabestelle durchgeführt werden. Diese würde dann ihren öffentlichen Schlüssel in der Smart Card speichern. Eine Kontrollstation würde dann zur Verifikation des Extraktes den von der Smart Card gelieferten öffentlichen Schlüssel der Ausgabestelle nutzen. Zur Verhinderung des Mißbrauches, etwa der Einspielung von gefälschten öffentlichen Schlüsseln einer Ausgabestelle, müssen die Schlüsselpaare der Ausgabestelle von einer zentralen Instanz elektronisch signiert werden. Ein solches Verfahren erlaubt die Ausgabe der Smart Card ohne Zugriff und Autorisierung durch ein Zentralsystem.

Jede Smart Card im System erhält bei der Herstellung eine eindeutige Seriennummer. Diese Seriennummer ist Grundlage der kryptographischen Verfahren, die aktiv durch die Smart Card ausgeführt werden. Die Smart Card enthält einen durch Ableitung der Seriennummer unter einem Masterschlüssel gewonnen smartcardspezifischen Schlüssel zur Authentisierung.

Die Authentisierung erfolgt implizit durch das Auslesen der Personendaten im sogenannten PRO-Mode. Der PRO-Mode ist eine in ISO7816 eingeführte Variante des Lesezugriffs, bei dem die an das Terminal übertragenen Daten durch einen Message Authentication Code (MAC) gesichert werden. Dieser MAC wird dynamisch bei jedem Lesezugriff neu erzeugt, um einen sogenannten Replay-Angriff, also das erneute Einspielen bereits gelesener Daten, auszuschließen.

Die Erzeugung des MAC erfolgt innerhalb des Betriebssystems der Smart Card unter Nutzung des kartenindividuellen Authentisierungsschlüssels und einer durch das Terminal gelieferten Zufallszahl. Das Terminal enthält hierzu in einem Sicherheitsmodul (z. B. eine weitere Smart Card) einen Zufallszahlengenerator und den Masterschlüssel, welche für die Ableitung des Smart Card-Schlüssels unter der Smart Card-Seriennummer benutzt wird. Das Terminal überprüft selbständig und unmittelbar nach dem Auslesen der Smart Card-Daten den MAC und weist eine Karte mit fehlerhaftem MAC ab.

Wichtig ist in diesem Zusammenhang, daß der MAC dynamisch durch die Smart Card erzeugt wird. Der dazu notwendige Schlüssel muß in der Smart Card vorhanden sein. Eine Manipulation der Smart Card, z. B. durch Duplizieren, erfordert Zugriff auf diesen Kartenschlüssel, welches nur unter hohem finanziellen Aufwand möglich ist.

Auch für diese Schutzstufe gibt es eine Variante, die jedoch eine leistungsfähigere Smart Card voraussetzt. Statt einem symmetrischen Verfahren für die MAC-Bildung (in der Regel Triple DES) kann das asymmetrische Verfahren der elliptischen Kurven Anwendung finden. Bei diesem Verfahren wird in der Karte der private, kartenindividuelle Schlüssel auslesegeschützt gespeichert und der öffentliche Schlüssel lesbar gemacht. Der öffentliche Schlüssel muß dazu mit dem privaten Schlüssel des Systembetreibers signiert werden. Ein Kontrollterminal braucht nun nur den weniger sicherheitskritischen, öffentlichen Schlüssel des Systembetreibers zu speichern und mit ihm die Echtheit des kartenindividuellen öffentlichen Schlüssel zu überprüfen.

Das Auslesen der Daten erfolgt analog dem symmetrischen Verfahren, mit der Abweichung, daß der MAC durch den asymmetrischen Algorithmus erzeugt wird.

Solche Verfahren auf Basis asymmetrischer Kryptographie finden aufgrund ihrer hohen Anforderungen an die Rechenleistung nur begrenzten Einsatz in Smart Cards. Im Detail muß hier sicher noch das Antwort-Zeitverhalten einer solchen Lösung betrachtet werden.

Die Übertragung der Daten zwischen Einrichtungen des Systems, insbesondere die Übertragung der Daten bei der Kartenausgabe soll durch kryptographische Verfahren abgesichert werden. Hierzu bieten sich Verfahren der Line-Verschlüsselung an, mit denen sich geschützte, transparente Datenkanäle aufbauen lassen.

Mit diesen Verfahren läßt sich die Integrität der Daten und die Vertraulichkeit sicherstellen. Letztere ist insbesondere bei der Erzeugung und Verteilung der Systemschlüssel von Bedeutung.

Ein wesentlicher, oft unterschätzter Mechanismus zur Sicherung von Informationssystemen ist die Einbettung der technischen Systeme in eine zuverlässige Ablauforganisation (5. Schale). Die besten und längsten Schlüsselverfahren der Welt nützen nichts, wenn die Schlüssel einfach zugänglich sind. Technische Verfahren können hier nur einen begrenzten Schutz herstellen, einem Angriff von innen sind sie oft schutzlos ausgeliefert.

Ein weiteres Merkmal der 5. Schale ist die Absicht, alle sicherheitsrelevanten Systemeinrichtungen in die Obhut der Grenzkontrollbehörde zu stellen. Dadurch soll aus Sicht der Behörde gewährleistet werden, daß ein Zugriff auf diese Systemeinrichtungen ohne ihr Zutun und unter keinen Umständen möglich ist. Dazu müssen sich nicht alle Systemeinrichtungen tatsächlich in den Räumlichkeiten der Behörde selbst befinden. Der technischen Betrieb könnte auch bei einem Beauftragten der Behörde durchgeführt werden, solange durch entsprechende vertragliche Gewährleistungsklauseln ein unerlaubter Zugriff durch Dritte (einschließlich dem Betreiber) unmöglich ist.

Eine zusätzliche organisatorische Schutzvorkehrung besteht darin, daß alle hoheitlichen Schritte – das heißt die Durchführung der vorgezogenen Grenzkontrolle entsprechend den nationalen, Schengener und EU-Anforderungen und die Freigabe der Smart Card – einem Beamten der Grenzkontrollbehörde vorbehalten sind. Für ihn sowie für die anderen Mitarbeiter in dem Enrolment Center bestehen geeignete Zugangskontrollen.

Darüber hinaus stellt die Erfassungssoftware sicher, daß Smart Cards

- nur auf der Basis im System bereits bekannter Smart Card-Rohlinge (jeder Smart Card-Rohling besitzt eine ein-eindeutige Kartennummer),
- nur mit Zutun im System legitimierter Grenzkontrollbeamter,
- nur nach erfolgreichem Durchlaufen aller erforderlichen Schritte und

nur für Angehörige bestimmter zugelassener Staaten ausgestellt werden, die im Besitz eines gültigen Reisedokumentes sind.

Die erfindungsgemäßen Systeme haben einige Vorteile, die es von verschiedenen anderen, bislang erfolglosen Versuchen zur flächendeckenden Einführung automatisierter Grenzkontrollen unterscheiden:

- Das System stellt eine wirksame und sparsame Möglichkeit dar, Grenzkontrollbehörden effizienter zu machen. Das System erlaubt es den Grenzkontrollkräften, sich auf einen eher polizeilich relevanten Personenkreis zu fokussieren. Damit können sie mit weniger Aufwand mehr für Sicherheit und Service leisten.
- Die gemäß einer besonderen Ausführungsform der Erfindung eingesetzte Smart Card erlaubt die Speicherung auch sensibler Daten ohne das Risiko eines Mißbrauchs durch unerlaubte Veränderungen oder von Fälschungen.
- Das Verfahren erlaubt kürzestmögliche Transaktionszeiten (im wesentlichen nur abhängig vom Antwort-Zeitverhalten der Abfrage bei der INPOL-Fahndungsdatenbank).
- Das Verfahren erlaubt geringstmögliche Transaktionskosten.
- Das Verfahren birgt keine datenschutzrechtliche Problematik (der Besitzer trägt seine vor unberechtigtem Zugriff sicher geschützten personenbezogenen Daten mit sich).
- Die in einer besonderen Ausführungsform der Erfindung verwendete Smart Card enthält ausreichende Speicherkapazität für diese und gegebenenfalls weitere zukünftige Anwendungen mit zusätzlichen Nutzpotentialen.

BNSDOCID: <DE_____19961403A1_I_>

- Auf der gemäß einer besonderen Ausführungsform der Erfindung verwendeten Smart Card befindet sich ausreichend Platz, um gegebenenfalls weitere Sicherheitsmerkmale (z. B. maschinenlesbares Hologramm mit Mikroschrift) oder andere Speichervarianten gleichzeitig zu nutzen.

Die in der vorstehenden Beschreibung, in den Zeichnungen sowie in den Ansprüchen offenbarten Merkmale der Erfindung können sowohl einzeln als auch in beliebigen Kombinationen für die Verwirklichung der Erfindung in ihren verschiedenen Ausführungsformen wesentliche sein.

Bezugszeichenliste

8 Grenze
10 Durchgangsschleuse
12 Eingang
14 Ausgang
16, 18 Drehtür
20 Kartenlesegerät
22 Biometriedatenlesegerät
24 Videokamera
26 Enrolment Center
28 Smart Card
30 dezentrales automatisiertes Grenzkontrollsystem
32 Dienststellen-Server
34 Fahndungsdatenbank
36 Trust Center
38 zentrale Datenverwaltungseinrichtung

Patentansprüche

1. System zur automatisierten Kontrolle des Passierens einer Grenze, mit:
- einer Einrichtung zur Erfassung von Personendaten von Systembenutzern,
- einer Einrichtung zur Erfassung von biometrischen Daten der Systembenutzer,
- einer Einrichtung zur Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank (**34**) und Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,
- einer Einrichtung zum Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,
- einer vor einer Grenze (**8**) angeordneten Durchgangsschleuse (**10**) zum Regulieren des Durchgangs der Systembenutzer mit einem Eingang (**12**) und einem Ausgang (**14**), wobei der Eingang (**12**) und der Ausgang (**14**) in Grundstellung verschlossen sind,
- einer vor dem Eingang (**12**) der Durchgangsschleuse (**10**) angeordneten Einrichtung zur Vereinzelung der Systembenutzer,
- einer hinter der Vereinzelungseinrichtung, aber vor dem Eingang (**12**) der Durchgangsschleuse (**10**) angeordneten Einrichtung zum Lesen der auf den Identifikationsmedien gespeicherten Daten,
- einer vor dem Eingang (**12**) der Durchgangsschleuse (**10**) angeordneten Einrichtung zur Überprüfung der Echtheit der Identifikationsmedien,
- einer vor dem Eingang (**12**) der Durchgangsschleuse (**10**) angeordneten Einrichtung zur Überprüfung des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- einer Einrichtung zum Öffnen des Eingangs (**12**) der Durchgangsschleuse (**10**), wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt wurden,
- einer in der Durchgangsschleuse (**10**) befindlichen Einrichtung zum Erfassen von biometrischen Daten eines hineingelassenen Systembenutzers,
- einer Einrichtung zum Vergleich der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- einer Einrichtung zum Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- einer Einrichtung zur Weitergabe der Personendaten an die Fahndungsdatenbank (**34**) und zur Abfrage, ob der Systembenutzer auf einer Fahndungsliste steht, und
- einer Einrichtung zum Öffnen des Ausgangs der Durchgangsschleuse (**10**) und Ermöglichen eines Grenzübertritts des Systembenutzers, wenn das Ergebnis der Fahndungsabfrage negativ ist, und zur Auslösung eines Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die Einrichtung zur Erfassung von Personendaten von Systembenutzern eine Einrichtung zum automatischen Einlesen der Personendaten aufweist.

3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Einrichtung zur Erfassung von biometrischen Daten eine Einrichtung zur Erfassung eines Fingerabdruckes und/oder der Netzhautstruktur und/oder der Gesichtsmerkmale und/oder der Stimme und/oder Sprache eines jeweiligen Systembenutzers aufweist.

4. System nach einem der Ansprüche 1 bis 3, gekennzeichnet durch eine Einrichtung zur Verarbeitung der erfaßten biometrischen Daten und Umrechnung in ein oder mehrere repräsentative(s) Datenmerkmal(e), anhand dessen/derer eine Wiedererkennung des Systembenutzers bei der Kontrolle möglich ist.

5. System nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Einrichtung zur Speicherung von Daten eine Einrichtung zur Verschlüsselung der Personen und/oder Identifikationsmediumdaten und zur Erzeugung eines identifikationsmediumspezifischen Schlüssels aufweist.

6. System nach Anspruch 5, dadurch gekennzeichnet, daß die Verschlüsselungseinrichtung ein lokal vorgesehenes Sicherheitsmodul ist oder sich in einem Hintergrundsystem befindet, das über eine On-Line-Datenverbindung verbunden ist.

7. System nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß die Einrichtung zur Speicherung der Daten eine Einrichtung zur elektrischen Personalisierung der verschlüsselten Daten in dem Identifikationsmedium und/oder eine Einrichtung zum Aufbringen der Personendaten und gegebenenfalls eines Fotos sowie der Unterschrift des jeweiligen Systembenutzers auf das Identifikationsmedium aufweist.

8. System nach Anspruch 7, dadurch gekennzeichnet, daß die Einrichtung zur Speicherung der Daten eine Einrichtung zum Überziehen des Identifikationsmedi-

BNSDOCID: <DE_____19961403A1_I_>

ums mit einer Laminatfolie aufweist.

9. System nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Identifikationsmedien Smart Cards (**28**) sind.

10. System nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß in der Durchgangsschleuse (**10**) mindestens eine Videokamera (**24**) vorgesehen ist.

11. System nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Einrichtung zum Lesen der auf den Identifikationsmedien gespeicherten Daten eine Einrichtung zum Berechnen des identifikationsmediumspezifischen Schlüssels aus den verschlüsselten Identifikationsmediumdaten und Verifikation desselben aufweist.

12. System nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Einrichtung zum Lesen der auf dem Identifikationsmedium gespeicherten Daten eine Einrichtung zum Entschlüsseln der verschlüsselten Personendaten und Verifikation derselben aufweist.

13. System nach einem der vorangehenden Ansprüche, gekennzeichnet durch eine Einrichtung zur Erzeugung und Verteilung von Schlüsseln für die Datenverschlüsselungen und Überwachung des Systembetriebes.

14. System nach einem der vorangehenden Ansprüche, gekennzeichnet durch eine Einrichtung zur Verwaltung und Überwachung insbesondere der Lebensdauer aller an Systembenutzer ausgegebener Identifikationsmedien.

15. System nach einem der vorangehenden Ansprüche, gekennzeichnet durch eine Einrichtung zur kryptographischen Verschlüsselung von zwischen Einrichtungen des Systems und/oder zwischen aus dem System und externen Einrichtungen übertragenen Daten.

16. Verfahren zur automatisierten Kontrolle des Passierens einer Grenze, das die folgenden Schritte umfaßt:

- Erfassen von Personendaten von Systembenutzern,
- Erfassen von biometrischen Daten der Systembenutzer,
- Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank und Vornahme einer Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,
- Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,
- Vereinzelung der einen Grenzübertrittsversuch unternehmenden Systembenutzer vor einer Durchgangsschleuse mit einem Eingang und einem Ausgang, wobei der Eingang und der Ausgang in Grundstellung geschlossen sind,
- Lesen der auf dem Identifikationsmedium gespeicherten Daten,
- Überprüfung der Echtheit des jeweiligen Identifikationsmediums,
- Überprüfen des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- Öffnen des Eingangs der Durchgangsschleuse, wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt werden,
- Erfassen von biometrischen Daten eines in die Durchgangsschleuse hineingelassenen Systembenutzers,
- Vergleichen der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- Weitergeben der Personendaten an die Fahndungsdatenbank und Abfragen, ob der Systembenutzer auf einer Fahndungsliste steht, und
- Öffnen des Ausgangs der Durchgangsschleuse, wenn das Ergebnis der Fahndungsabfrage negativ ist, bzw. Auslösen eine Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, daß die Personendaten der Systembenutzer durch automatisches Einlesen erfaßt werden.

18. Verfahren nach Anspruch 16 oder 17, dadurch gekennzeichnet, daß der Fingerabdruck und/oder die Netzhautstruktur und/oder die Gesichtsmerkmale und/oder die Stimme und/oder die Sprache eines jeweiligen Systembenutzers erfaßt wird/werden.

19. Verfahren nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, daß die erfaßten biometrischen Daten verarbeitet und in einer oder mehrere repräsentative(s) Datenmerkmal(e) umgerechnet werden, anhand dessen/derer eine Wiedererkennung des Systembenutzers bei der Kontrolle möglich ist.

20. Verfahren nach einem der Ansprüche 16 bis 19, dadurch gekennzeichnet, daß die Personen- und/oder Identifikationsmediumdaten verschlüsselt werden und ein identifikationsmediumspezifischer Schlüssel erzeugt wird.

21. Verfahren nach einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, daß die verschlüsselten Daten in dem Identifikationsmedium elektrische personalisiert und/oder die Personendaten und gegebenenfalls ein Foto sowie Unterschriften des jeweiligen Systembenutzers auf das Identifikationsmedium aufgebracht werden.

22. Verfahren nach einem der Ansprüche 16 bis 21, dadurch gekennzeichnet, daß die Identifikationsmedien mit einer Laminatfolie überzogen werden.

23. Verfahren nach einem der Ansprüche 16 bis 22, dadurch gekennzeichnet, daß als Identifikationsmedium Smart Cards verwendet werden.

24. Verfahren nach einem der Ansprüche 16 bis 23, dadurch gekennzeichnet, daß die Durchgangsschleuse mittels einer Videokamera überwacht wird.

25. Verfahren nach einem der Ansprüche 16 bis 24, dadurch gekennzeichnet, daß aus den verschlüsselten Identifikationsmediumdaten ein identifikationsmediumspezifischer Schlüssel berechnet und verifiziert wird.

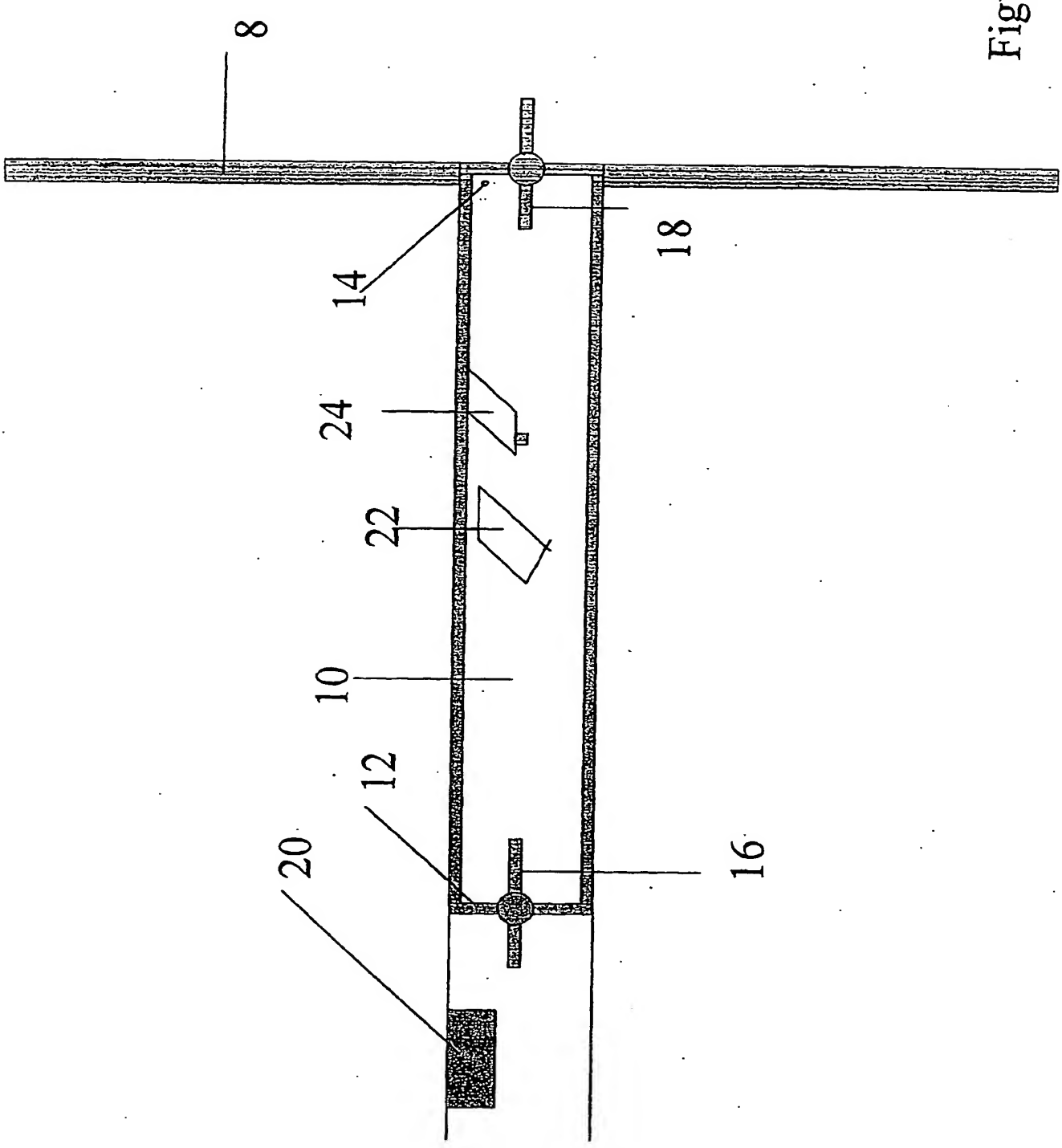
26. Verfahren nach einem der Ansprüche 16 bis 25, dadurch gekennzeichnet, daß die verschlüsselten Personendaten entschlüsselt und verifiziert werden.

Hierzu 2 Seite(n) Zeichnungen

BNSDOCID: <DE_____19961403A1_I_>

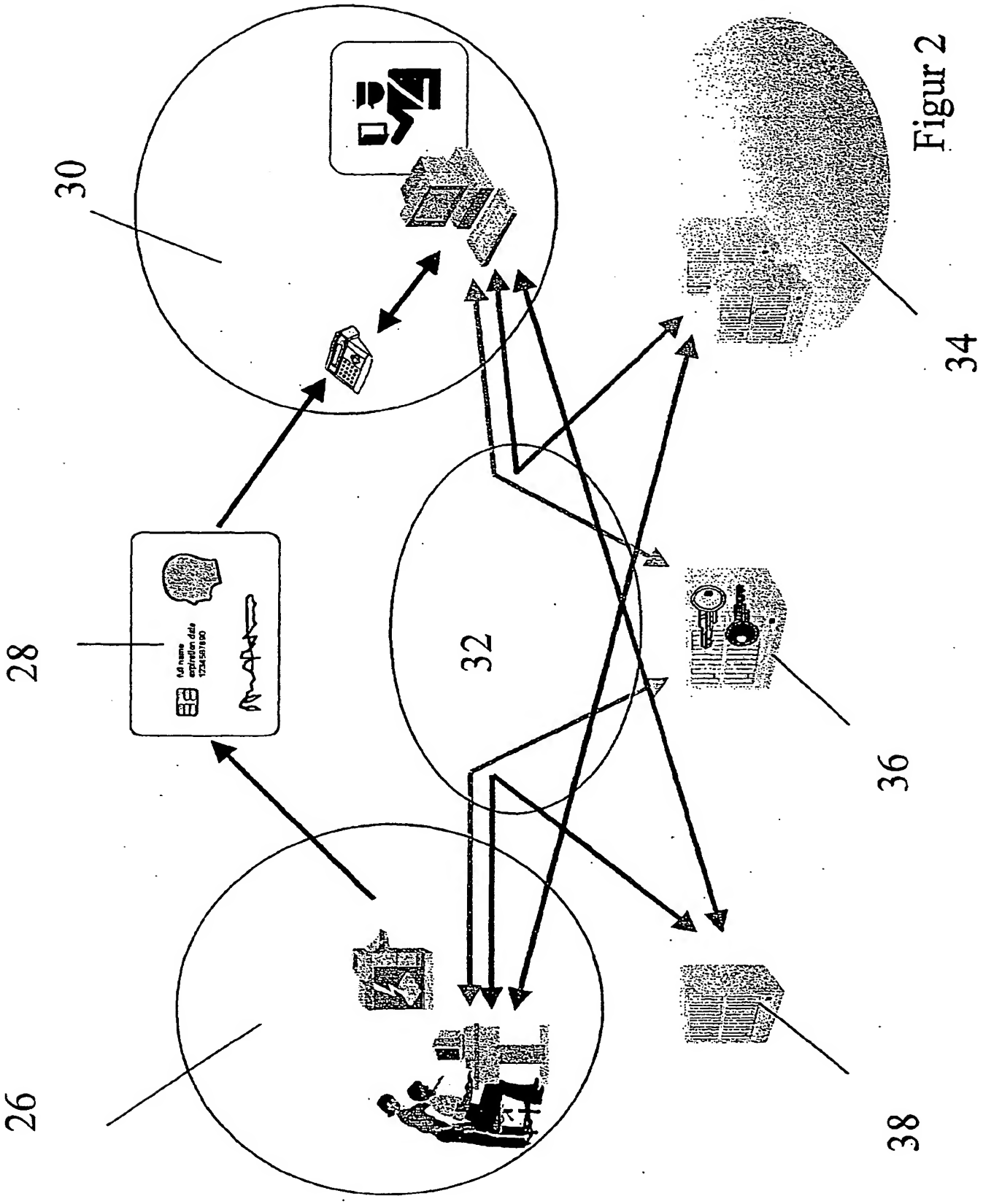
Nummer: DE 199 61 403 A1
Int. Cl.[7]: G 07 C 9/00
Offenlegungstag: 2. August 2001

Figur 1



BNSDOCID: <DE_____19961403A1_I_>

Nummer: DE 199 61 403 A1
Int. Cl.[7]: G 07 C 9/00
Offenlegungstag: 2. August 2001



Figur 2

BNSDOCID: <DE_____19961403A1_I_>